

WHAT IS CLAIMED IS:

1 1. A method for clustered Secure Sockets Layer (SSL) acceleration
2 comprising:
3 connecting at least two SSL relays in a cluster;
4 transferring information between a first node and one of the at least two SSL
5 relays, the transferred information related to communication between the first node
6 and a second node; and
7 clustering state information of an SSL connection between the first node and
8 the one of the at least two SSL relays, the clustering comprising sharing the state
9 information between one of the at least two SSL relays and all other SSL relays in
10 the cluster, wherein any of the at least two SSL relays can take over all connections
11 of another of the at least two SSL relays, therefore providing no interruption in the
12 communication should any of the at least two SSL relays fail.

1 2. The method according to claim 1, wherein the first node comprises a client
2 and the second node comprises a server.

1 3. The method according to claim 1, further comprising transferring the
2 information between the first node and a second of the at least two clustered SSL
3 relays transparently to the first node upon failure of the one at least two SSL relays.

1 4. The method according to claim 1, further comprising transferring the
2 communication from the first node to a second of the at least two clustered SSL
3 relays and from the second of the at least two SSL relays to the second node
4 transparently to the first node upon failure of the one at least two SSL relays.

1 5. The method according to claim 1, wherein the communication comprises
2 data being transferred between the first node and the second node.

1 6. The method according to claim 5, further comprising transferring the data
2 between the first node and the second node through a second at least two SSL
3 relays transparently to the client upon failure of the first at least two SSL relays.

1 7. The method according to claim 1, further comprising sharing an SSL
2 session cache across all of the at least two SSL relays.

1 8. The method according to claim 1, further comprising clustering an SSL
2 session resumption between the first node and the one of the at least two SSL
3 relays.
4

1 9. The method according to claim 1, further comprising clustering
2 cryptographic keying information across all of the at least two SSL relays.

1 10. The method according to claim 9, further comprising clustering a key and
2 a current Cipher Block Chaining (CBC) residue.

1 11. The method according to claim 9, further comprising clustering a
2 sequence number.

1 12. The method according to claim 9, further comprising clustering a current
2 key schedule.

13. The method according to claim 9, further comprising clustering a key and an offset into a key stream.

14. The method according to claim 1, further comprising clustering a cipher state.

15. The method according to claim 1, further comprising clustering data from a partial record corresponding to data from either the first or second node.

16. The method according to claim 1, further comprising clustering a record size before the record is transmitted.

17. A system for clustered Secure Sockets Layer (SSL) acceleration comprising:

a first node;

at least two SSL relays connected in a cluster, the cluster operatively connected to the first node; and

a second node operatively connected to the at least two clustered SSL relays, one at least two clustered SSL relays transferring information between the first node and the second node,

wherein the state information of an SSL connection between the first node and the one at least two SSL relays is shared across each of the at least two SSL relays, such that any of the at least two SSL relays is capable of taking over all connections of another of the at least two SSL relays therefore providing no interruption in the transfer of information should any of the at least two SSL relays fail.

1 18. The system according to claim 17, wherein the first node is a client and
2 the second node is a server.

1 19. An apparatus comprising a storage medium containing instructions stored
2 therein, the instructions when executed causing a computing device to perform:
3 connecting the computing device with at least one other computing device in a
4 cluster;
5 transferring information between a first node and the computing device, the
6 transferred information related to communication between the first node and a
7 second node; and
8 clustering the state information of a connection between the first node and the
9 computing device, the clustering comprising sharing the state information with each
10 of the at least one other computing device, wherein any of the computing devices
11 can take over all connections of another computing device, therefore providing no
12 interruption in the communication should any of the computing devices fail

1 20. The apparatus according to claim 19, wherein each computing device
2 comprises a Secure Sockets Layer (SSL) relay.

1 21. The apparatus according to claim 19, wherein the first node is a client
2 and the second node is a server.

1 22. An SSL relay, the SSL relay connected in a cluster of SSL relays,
2 comprising:
3 a first interface for transferring information between a first node and the SSL
4 relay;

5 a second interface for transferring information between a second node and
6 the SSL relay;
7 a third interface for transferring information between SSL relays in the cluster;
8 and
9 a storage device, wherein the state information of an SSL connection between
10 the first node and the SSL relay is shared across each SSL relay in the cluster, any
11 of the SSL relays in the cluster capable of taking over all connections of another SSL
12 relay in the cluster, therefore providing no interruption in the transfer of information
13 should any of the SSL relays in the cluster fail.

1 23. The apparatus according to claim 22, wherein the first node is a client
2 and the second node is a server.

1 24. The apparatus according to claim 22, wherein the first interface and the
2 second interface are the same.

1 25. The apparatus according to claim 22, wherein the second interface and
2 the third interface are the same.

1 26. The apparatus according to claim 22, wherein the first interface and the
2 third interface are the same.

1 27. The apparatus according to claim 22, wherein the first interface and the
2 second interface and the third interface are the same.